UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MATTHEW BRACKMAN, individually and on behalf of all others similarly situated, Plaintiff, v. T-MOBILE USA, INC., Defendant.	CLASS ACTION Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Matthew Brackman ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant") stemming from a recent data breach and the theft of Personal Identifying Information ("PII"), including Social Security Numbers, dates of birth, and drivers' license numbers, belonging to tens-of-millions of Defendant's customers nationwide.

JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

proposed Class members. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367 because they form part of the same case or controversy as the claims within the Court's original jurisdiction.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiff's claims arise out of Defendant's contacts with this district.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

PARTIES

4. Plaintiff Matthew Brackman is a resident and citizen of the state of Ohio.

5. Defendant T-Mobile USA, Inc. is a Delaware corporation with its principal place of business in Bellevue, Washington.

FACTUAL ALLEGATIONS

I. T-Mobile USA, Inc.

6. Defendant is a multinational telecommunications company that provides mobile phone services and other services throughout the United States and the world.

7. Defendant has over 102.1 million customers.[1]

8. Customers, like Plaintiff and Class members, provide certain Personal Identifying Information ("PII") to Defendant which is required in order to obtain mobile phone services and other services. This information includes:

[1] https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2021/T-Mobile-Adds-5.5-Million-Postpaid-Customers-in-2020--the-Most-in-Company-History--and-Further-Expands-5G-Network-Leadership-by-Exceeding-Ambitious-2020-5G-Goals/default.aspx.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

a. Name;

b. Address;

c. Phone number;

d. Driver's license number;

e. Social Security number;

f. Financial information;

g. Government identification number; and

h. Date of birth.

9. As a technology company with an acute interest in maintaining the confidentiality of the PII entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding users' PII.

10. Defendant represents to its customers that it possesses robust security features to protect PII. Defendant assures Plaintiffs and Class Members, "With T-Mobile, you don't have to worry. Our privacy principles mean you can trust us to do the right thing with your data."[2]

11. Defendant also represents:

> We use administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control. For example, when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access.
>
> Despite our efforts, we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use, or disclose personal data. Be sure to use a strong password to access your information and not one you use for other services. You should also use multi-factor authentication where possible.[3]

II. The Value of Personal Identifying Information

[2] https://www.t-mobile.com/privacy-center.

[3] https://www.t-mobile.com/privacy-center/our-practices/privacy-policy.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

12. It is well known that PII, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

13. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[4]

14. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[5]

15. Consumers are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[6] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[7]

16. The PII of minors (like the dependents of many Class Members) can be used to receive illicit gains through methods such as credit card fraud with newly created accounts. The

---

[4] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[5] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[6] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[7] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

fact that a minor's social security number has not yet been used for financial purposes actually makes it more valued by hackers rather than less. The "blank slate" credit file of a child is much less limited than the potentially low credit score of an adult. Social security numbers that have never been used for financial purposes are uniquely valuable as thieves can pair them with any name and birthdate. After that happens, thieves can open illicit credit cards or even sign up for government benefits.[8]

III. Industry Standards for Data Security

17. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Capital One, Marriott, and Equifax, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

18. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

[8] Richard Power, "Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers," Carnegie Mellon CyLab, https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

i. Monitoring for server requests from Tor exit nodes.

19. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[9] and protection of PII[10] which includes basic security standards applicable to all types of businesses.

20. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to

[9] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[10] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

21. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[11]

22. Because Defendant was entrusted with applicants' PII, it had, and has, a duty to applicants to keep their PII secure.

23. Applicants, such as Plaintiff and the Class, reasonably expect that when they provide PII to a company, the company will safeguard their PII.

24. Nonetheless, Defendant failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the data breach discussed below. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the data breach.

IV. The Data Breach

[11] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

25. On August 15, 2021, Defendant stated that it was investigating "a forum post claiming to be selling a mountain of personal data." The seller stated that "they have obtained data related to over 100 million people, and that the data came from T-Mobile servers."[12]

26. The seller stated that "[t]he data includes social security numbers, phone numbers, names, physical addresses, unique IMEI numbers, and driver licenses information."[13]

27. The asking price for a subset of the data containing 30 million Social Security numbers was 6 bitcoin, worth approximately $270,000.[14]

28. On August 16, 2021, Defendant acknowledged that "unauthorized access to some T-Mobile data occurred."[15]

29. Defendant also stated, "We are confident that the entry point used to gain access has been closed."[16]

30. On August 17, 2021, Defendant confirmed that "a subset of T-Mobile data had been accessed by unauthorized individuals," including "customers' first and last names, date of birth, SSN, and driver's license/ID information for a subset of current and former postpay customers and prospective T-Mobile customers."[17]

31. Defendant stated that it would send communications to affected customers stating that it is:

- Immediately offering 2 years of free identity protection services with McAfee's ID Theft Protection Service.

---

[12] https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million.

[13] *Id.*

[14] *Id.*

[15] https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021.

[16] *Id.*

[17] https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

- Recommending all T-Mobile postpaid customers proactively change their PIN by going online into their T-Mobile account or calling our Customer Care team by dialing 611 on your phone. This precaution is despite the fact that we have no knowledge that any postpaid account PINs were compromised.

- Offering an extra step to protect your mobile account with our Account Takeover Protection capabilities for postpaid customers, which makes it harder for customer accounts to be fraudulently ported out and stolen.

- Publishing a unique web page later on Wednesday for one stop information and solutions to help customers take steps to further protect themselves.[18]

32. Plaintiff received a letter from Defendant dated September 2, 2021, notifying them of the breach and advising them to "remain vigilant against threats of identity theft or fraud, and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity."

33. Plaintiff also received a text message from Defendant notifying them of the breach.

34. Defendant did not state how long the unauthorized individuals had access to Defendant's servers or when the breach first occurred.

35. Defendant did not state why it was unable to detect the unauthorized individuals accessing Defendant's servers.

36. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

[18] *Id.*

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

37. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiffs' PII, Plaintiff and the Class have been damaged.

38. Plaintiffs and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages in order to prevent and mitigate credit fraud or identity theft. The information exposed in the data breach is, by its very nature, the information necessary to obtain mobile phone services, apply for and obtain lines of credit, and myriad financially related activities.

39. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[19]

40. In addition to fraudulent charges and damage to their credit, Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as

[19] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

41. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value and/or use of their PII entrusted to Defendant, and loss of privacy.

CLASS ALLEGATIONS

42. Plaintiff, individually and on behalf of all others, brings this class action pursuant to Fed. R. Civ. P. 23.

43. The proposed Class is defined as follows:

> **Nationwide Class:** All persons who utilized Defendant T-Mobile USA, Inc.'s services and whose PII was maintained on Defendant T-Mobile USA, Inc.'s servers that were compromised in the Data Breach.

44. The Class excludes the following: Defendant, its affiliates, and its current and former employees, officers and directors, and the Judge assigned to this case.

45. Plaintiffs reserve the right to modify, change, or expand the definitions of the proposed Class based upon discovery and further investigation.

46. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, Plaintiff reasonably approximates that the number of Class Members is in excess of 53 million.[20] The Class Members can be readily identified through Defendant's records.

47. *Commonality*: Questions of law or fact common to the Class include, without limitation:

[20] *See* https://www.foxbusiness.com/technology/t-mobile-hit-with-class-action-lawsuits-over-data-breach.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

a. Whether Defendant owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class' PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class' PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

48. *Typicality*: The claims or defenses of Plaintiffs are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

49. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiff has retained

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

50. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as whether Defendant owed a duty to Plaintiff and the Class and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

51. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

52. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

53. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

54. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

55. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(on behalf of the Class)

56. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

57. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiff and other Class members would be harmed by such exposure of their PII.

58. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

members, on the other hand. The special relationship arose because Plaintiff and Class members entrusted Defendant with their PII as part of the process to obtain mobile phone services. Defendant alone could have ensured that its data security systems and practices were sufficient to prevent or minimize the data breach.

59. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

60. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

61. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII.

62. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII within its possession, custody, and control.

63. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

64. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the breach.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

65. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

66. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

67. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised.

68. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of two years. Defendant is also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and the Class have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and the Class to the extent their PII has been diminished in value because Plaintiff and the Class no longer control their PII and to whom it is disseminated.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

COUNT II
INVASION OF PRIVACY
(on behalf of the Class)

69. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

70. Defendant invaded Plaintiff's and the Class's right to privacy by allowing the unauthorized access to their PII and by negligently maintaining the confidentiality of Plaintiff's and the Class's PII, as set forth above.

71. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII was disclosed without prior written authorization from Plaintiff and the Class.

72. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class provided and disclosed their PII to Defendant privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

73. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class' PII was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class suffered damages as described herein.

74. Defendant committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII with a willful and conscious disregard of their right to privacy.

75. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class great and irreparable injury in

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and the Class's PII with sub-standard and insufficient protections.

COUNT III
UNJUST ENRICHMENT
(on behalf of the Class)

76. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

77. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

78. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiff's and the Class's PII.

79. Defendant also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

80. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and the Class. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiff and the Class. The benefits conferred upon, received, and enjoyed by Defendant

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

81. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII, Plaintiff and the Class suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

82. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and the Class, wherein it profited from interference with Plaintiff's and the Class's legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

83. Accordingly, Plaintiff, on behalf of himself and the Class, respectfully requests that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII, and/or compensatory damages.

COUNT IV
BAILMENT
(on behalf of the Class)

84. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

85. Plaintiff and the Class provided, or authorized disclosure of, their PII to Defendant for the exclusive purpose of obtaining mobile phone services.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

86. In allowing their PII to be made available to Defendant, Plaintiff and the Class intended and understood that Defendant would adequately safeguard their PII.

87. For its own benefit, Defendant accepted possession of Plaintiff's and the Class's PII for the purpose of making available its own services.

88. By accepting possession of Plaintiff's and the Class's PII, Defendant understood that Plaintiff and the Class expected Defendant to adequately safeguard their personal information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Defendant owed a duty to Plaintiff and the Class to exercise reasonable care, diligence, and prudence in protecting their personal information.

89. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and the Class's personal information, resulting in the unlawful and unauthorized access to and misuse of their PII.

90. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs and Class Members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth above.

91. As a direct and proximate result of Defendant's breach of its duties, the personal information of Plaintiff and the Class entrusted, directly or indirectly, to Defendant during the bailment (or deposit) was damaged and its value diminished.

COUNT V
BREACH OF IMPLIED CONTRACT
(on behalf of the Class)

92. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

93. Defendant invited applicants, including Plaintiff and the Class, to obtain mobile phone services. As consideration for the benefits Defendant was to administer, Plaintiff and the Class provided their PII to Defendant. When Plaintiff and the Class provided their PII to Defendant, they entered into implied contracts by which Defendant agreed to protect their PII and only use it solely to administer benefits. As part of the offer, Defendant would safeguard the PII using reasonable or industry-standard means.

94. Accordingly, Plaintiff and the Class accepted Defendant's offer to provide mobile phone services and provided Defendant their PII.

95. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant. However, Defendant breached the implied contracts by failing to safeguard Plaintiff's and the Class's PII.

96. The losses and damages Plaintiff and the Class sustained that are described herein were the direct and proximate result of Defendant's breaches of its implied contracts with them. Additionally, because Plaintiff and the Class continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiff and the Class are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII from unlawful exposure.

97. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and Defendant is liable to Plaintiff and the Class for associated damages and specific performance.

COUNT VI
BREACH OF CONFIDENCE
(on behalf of the Class)

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

98. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

99. As alleged above, Plaintiff and the Class had agreements with Defendant, both express and implied, that required Defendant to keep their PII confidential.

100. Defendant breached that confidence by disclosing Plaintiff's and the Class's PII without their authorization and for unnecessary purposes.

101. As a result of the data breach, Plaintiff and the Class suffered damages that were attributable to Defendant's failure to maintain confidence in their PII.

COUNT VII
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
Wash. Rev. Code Ann. § 19.86.010 *et seq.*
(on behalf of the Class)

102. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

103. Plaintiff and the Class are "persons" within the meaning of Wash. Rev. Code Ann. § 19.86.010(1).

104. Defendant is a "person" within the meaning of the Wash. Rev. Code Ann. § 19.86.010(1), and Defendant conducts "trade" and "commerce" within the meaning of Wash. Rev. Code Ann. § 19.86.010(2).

105. Wash. Rev. Code Ann. § 19.86.020 states: "Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

106. Defendant's conduct, as described above, constitutes unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

107. Defendant's conduct directly and proximately caused injury to Plaintiff and the Class.

108. Defendant's conduct is injurious to the public interest because it "(a) [i]njured other persons; (b) had the capacity to injure other persons; [and] (c) has the capacity to injure other persons." Wash. Rev. Code Ann. § 19.86.093.

109. Wash. Rev. Code Ann. § 19.86.090 states: "Any person who is injured in his or her business or property by a violation of RCW 19.86.020 . . . may bring a civil action in superior court to enjoin further violations, to recover the actual damages sustained by him or her, or both, together with the costs of the suit, including a reasonable attorney's fee."

110. As a direct and proximate result of Defendant's unfair acts and / or practices, Plaintiff and the Class suffered injury in fact and actual damages including, but not limited to, the lost value of their PII, ongoing and imminent and certainly impending threat of identity theft and fraud, time spent monitoring and reviewing bank and credit card statements, initiating fraud alerts and identify theft alerts, lost work time, and other damages.

111. Plaintiff and the Class are entitled to (1) an order enjoining the conduct described above and ordering Defendant to take remedial measures to prevent future breaches, (2) actual damages, (3) treble damages pursuant to RCW §19.86.090; and (4) costs and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury.

Dated: September 21, 2021.

s/Matthew J. Ide, WSBA No. 26002
Matthew J. Ide, WSBA No. 26002
IDE LAW OFFICE
7900 SE 28th Street, Suite 500
Mercer Island, WA 98040
Tel. (206) 625-1326
Fax: (206) 622-0909
email: mjide@yahoo.com

Charles Schaffer, Esq.*
Nicholas J. Elia, Esq.*
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106-3697
Telephone: (215) 592-1500
dlevin@lfsblaw.com
nelia@lfsblaw.com

Jeffrey S. Goldenberg, Esq.*
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Telephone: (513) 345-8291
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

Joseph Lyon, Esq.*
THE LYON FIRM, LLC
2754 Erie Ave
Cincinnati, OH 45208
Telephone: (513) 381-2333

jlyon@thelyonfirm.com

Attorneys for Plaintiff

* Denotes pro hac vice motion to be filed.

IDE LAW OFFICE
7900 SE 28TH STREET, SUITE 500
MERCER ISLAND, WA 98040
PH.: 206 625-1326